

Appl. No. 10/803,945

Amendment

Response to Office Action mailed August 28, 2007

RECEIVED  
CENTRAL FAX CENTER

NOV 28 2007

Docket No. TSM-37

**AMENDMENTS TO THE CLAIMS**

This listing of claims replaces all prior versions and listings of claims in the application:

**LISTING OF CLAIMS:**

1-6. (Canceled)

7. (Previously Presented) In a computer system including a host computer coupled to and separate from a storage system which has a first volume for storing data received from the host computer and a second volume that is a pair of said first volume and that stores data that is replicated from said first volume, and a storage control unit for controlling the data replication from the first volume to said second volume, a data protection apparatus coupled to and separate from the host computer and the storage system, comprising:

an event detection unit for detecting an event occurrence;

a replication stopping unit for instructing said storage control unit to stop the replication of data of said first volume to said second volume, when said event detection unit detects an event; and

an illegal intrusion detection unit for detecting an illegal intrusion into said host computer;

wherein said event detection unit receives a detection of the illegal intrusion from said illegal intrusion detection unit; and

Appl. No. 10/803,945

Docket No. TSM-37

Amendment

Response to Office Action mailed August 28, 2007

when said event detection unit receives the detection of the illegal intrusion, said replication stopping unit instructs said storage control unit to stop data replication from said first volume to said second volume that is the pair of said first volume.

8. (Cancelled)

9. (Previously Presented) A data protection apparatus in a computer system according to Claim 7, wherein:

said computer system further includes a computer virus detection unit for detecting a computer virus in said storage system;

said event detection unit receives the detection of the computer virus from said computer virus detection unit; and

when said event detection unit receives the detection of the computer virus, said replication stopping unit instructs said storage control unit to stop data replication from said first volume to said second volume that is the pair of said first volume.

10. (Previously Presented) A data protection method for protecting data in a computer system including a host computer coupled to and separate from a storage system which has a first volume for storing data received from the host computer and a second volume that is a pair of said first volume and that stores data that is replicated from said first volume, and a storage control unit coupled to and separate from said storage system for

Appl. No. 10/803,945

Docket No. TSM-37

Amendment

Response to Office Action mailed August 28, 2007

controlling data replication from said first volume to said second volume, wherein said data protection method comprises steps of:

detecting an intrusion into said host computer; and  
instructing said storage control unit to stop data replication from said first volume to said second volume when said intrusion is detected.

11. (Previously Presented) A program embodied on a storage medium that can be read by an information processing apparatus for making the information processing apparatus perform data protection in a computer system including a host computer coupled to and separate from a storage system which has a first volume for storing data received from the host computer and a second volume that is a pair of said first volume and that stores data that is replicated from said first volume, and a storage control unit coupled to and separate from said storage system for controlling data replication from said first volume to said second volume, wherein said program makes said information processing apparatus perform processes of:

detecting that an intrusion into the host computer has occurred; and  
instructing said storage control unit to stop data replication from said first volume to said second volume when said intrusion is detected.

12-13. (Canceled)

Appl. No. 10/803,945

Docket No. TSM-37

Amendment

Response to Office Action mailed August 28, 2007

14. (Previously Presented) In a computer system including a host computer coupled to and separate from a storage system which has a first volume for storing data received from the host computer and a second volume that is a pair of said first volume and that stores data that is replicated from said first volume, and a storage control unit coupled to and separate from said storage system for controlling data replication from the first volume to said second volume, a data protection apparatus coupled to and separate from the host computer and the storage apparatus comprising:

an event detection unit for detecting an event occurrence; and

a replication stopping unit for instructing said storage control unit to stop data replication from said first volume to said second volume when said event detection unit detects an event;

wherein said computer system further comprises an alteration detection unit that reads given data in a plurality of said second volumes to detect respective differences between the given data; and

the event detected by said event detection unit is a detection result of the differences between the given data, with said detection result being received from said alteration detection unit.

15. (Previously Presented) A data protection apparatus in a computer system according to Claim 14, wherein:

Appl. No. 10/803,945

Docket No. TSM-37

Amendment

Response to Office Action mailed August 28, 2007

write data to said first volume is replicated by said storage control unit to said second volume with a delay of a given time.

16. (Previously Presented) A data protection apparatus in a computer system

according to Claim 14, wherein:

as said second volume, a plurality of second volumes are provided; and

said storage control unit switches a replication destination of write data of said first volume, at given time intervals among said plurality of second volumes.

17. (Previously Presented) A data protection apparatus in a computer system

according to Claim 16, wherein:

data replicated to said plurality of second volumes is further replicated to another plurality of said second volumes.

18. (Canceled)

19. (Previously Presented) A data protection apparatus in a computer system

according to Claim 14, wherein:

said storage control unit further controls communication between said host computer and said first volume; and

Appl. No. 10/803,945

Docket No. TSM-37

Amendment

Response to Office Action mailed August 28, 2007

said data protection apparatus instructs said storage controller to stop communication between said host computer and said first volume when said event detection unit detects said event.

20. (Cancelled)

21. (Previously Presented) A data protection apparatus in a computer system according to Claim 7, wherein said replication stopping unit further instructs said storage control unit to cancel data replication from said first volume to said second volume.

22. (Previously Presented) A data protection apparatus in a computer system according to Claim 7, further including a path disconnection unit for instructing said storage control unit to stop communication between said host computer and said storage system, when said event detection unit detects an event.

23. (Previously Presented) A data protection method according to Claim 10, further including the step of instructing said storage control unit to cancel data replication from said first volume to said second volume that is the pair of said first volume, when said intrusion is detected

Appl. No. 10/803,945

Docket No. TSM-37

Amendment

Response to Office Action mailed August 28, 2007

24. (Previously Presented) A data protection method according to Claim 10, further including the step of instructing said storage control unit to stop communication between said host computer and said storage system, when said intrusion is detected.

25. (Previously Presented) A program embodied on a storage medium according to Claim 11, further including said program making said information processing apparatus perform the process of instructing said storage control unit to cancel data replication from said first volume to said second volume that is the pair of said first volume, when said intrusion is detected

26. (Previously Presented) A program embodied on a storage medium according to Claim 11, further including said program making said information processing apparatus perform the process of instructing said storage control unit to stop communication between said host computer and said storage system, when said intrusion is detected.

27. (Previously Presented) A data protection apparatus in a computer system according to Claim 14, wherein said replication stopping unit further instructs said storage control unit to cancel data replication from said first volume to said second volume.

28. (Previously Presented) A data protection apparatus in a computer system according to Claim 7, further including a path disconnection unit for instructing said storage control unit

Appl. No. 10/803,945

Docket No. TSM-37

Amendment

Response to Office Action mailed August 28, 2007

to stop communication between said host computer and said storage system, when said event detection unit detects an event.